07 - 24 - 00   A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
APPLICATION TRANSMITTAL LETTER FOR
NONPROVISIONAL PATENT APPLICATION
Under 37 C.F.R. 1.53(b)

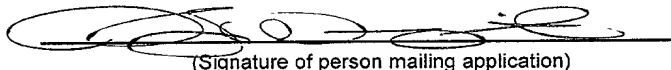Certification under 37 CFR 1.10 (if applicable)

EL447059720US
EXPRESS MAIL mailing number

July 21, 2000
Date of Deposit

I hereby certify that this application is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, DC 20231.

Dana J. Warnquist
(Type or printed name of person mailing application)

(Signature of person mailing application)

Assistant Commissioner for Patents
Washington, DC   20231

Sir:

Transmitted herewith for filing is the patent application, including 7 sheets of formal/informal drawings, of inventors: **Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, Thomas H. James** for: **VIDEO ON DEMAND PAY PER VIEW SERVICES WITH UNMODIFIED CONDITIONAL ACCESS FUNCTIONALITY**

The filing fee for this application is calculated below:

	CLAIMS AS FILED						
	NUMBER FILED	NUMBER EXTRA		RATE			
Basic Fee						$	0.00
Total Claims	37	-20 =	17	x	$ 18.00	$	0.00
Independent Claims	3	- 3 =	3	x	$ 78.00	$	0.00
Multiple Dependent Claims				+	$260.00	$	0.00
TOTAL FILING FEE :						$	0.00

Please charge Deposit Account No. 50-0383 of Hughes Electronics Corporation, El Segundo, California, in the amount of **$0.00**. The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to that account.

The Commissioner is further hereby authorized to charge to said above Deposit Account No. 50-0383, pursuant to 37 CFR 1.25(b), any fees whatsoever which may properly become due or payable, as set forth in 37 CFR 1.16 to 1.17 inclusive, for the entire pendency of this application without specific additional authorization.

Please associate this application with the Hughes Electronics Corporation Customer Number 020991.

This form is submitted in triplicate.

HUGHES ELECTRONICS CORPORATION

John A. Crook, Registration No.: 30,830
Attorney for Applicants

CUSTOMER NUMBER 020991
HUGHES ELECTRONICS CORPORATION
Bldg. 001, M/S A109
PO Box 956
El Segundo, CA   90245-0956
Telephone: 303/712.5044
Date: July 21, 2000

09-506 (7/98)

VIDEO ON DEMAND PAY PER VIEW SERVICES WITH UNMODIFIED CONDITIONAL ACCESS FUNCTIONALITY

Inventors:

Raynold M. Kahn
Gregory J. Gagnon
David D. Ha
Peter M. Klauss
Christopher P. Curren
Thomas H. James

VIDEO ON DEMAND PAY PER VIEW SERVICES WITH UNMODIFIED CONDITIONAL ACCESS FUNCTIONALITY

CROSS-REFERENCE TO RELATED APPLICATIONS

5   This application is related to the following patent applications, all of which applications are hereby incorporated by reference herein:

U.S. Patent Application Serial No. --/---,---, entitled "SECURE STORAGE AND REPLAY OF MEDIA PROGRAMS USING A HARD-PAIRED RECEIVER AND STORAGE DEVICE," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M.

10   Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200042, filed on same date herewith;

U.S. Patent Application Serial No. --/---,---, entitled "SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS IN A HARD-PAIRED RECEIVER AND STORAGE DEVICE," by Raynold M. Kahn, Gregory J. Gagnon,

15   David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200043, filed on same date herewith;

U.S. Patent Application Serial No. --/---,---, entitled "SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH MODIFIED CONDITIONAL ACCESS FUNCTIONALITY, " by Raynold M. Kahn, Gregory J.

20   Gagnon, David D. Ha, Peter M. Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-20044, filed on same date herewith;

U.S. Patent Application Serial No. --/---,---, entitled "SUPER ENCRYPTED STORAGE AND RETRIEVAL OF MEDIA PROGRAMS WITH SMARTCARD GENERATED KEYS," by Raynold M. Kahn, Gregory J. Gagnon, David D. Ha, Peter M.

25   Klauss, Christopher P. Curren, and Thomas H. James, attorney's docket number PD-200045, filed on same date herewith; and

U.S. Patent Application Serial No. 09/491,959, entitled "VIRTUAL VIDEO ON DEMAND USING MULTIPLE ENCRYPTED VIDEO SEGMENTS," by Robert G. Arsenault and Leon J. Stanger, attorney's docket number PD-980208, filed on January 26,

30   2000.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to systems and methods for providing video program material to subscribers, and in particular to a method and system for securely storing and
5   replaying media programs.

2. Description of the Related Art

In recent years, there has been increasing interest in allowing cable and satellite television subscribers to record broadcast media programs for later viewing. This
10   capability, hereinafter referred to as personal video recording (PVR), can be used to provide video-on-demand (VOD) services, or simply to allow the subscriber to save media programs for repeated viewing and/or archival purposes.

In the past, video cassette tape recorders (VCRs) have been used for such personal video recording. Recently, however, hard disks, similar to those used in personal
15   computers, have been used to store media programs for later viewing. Unlike VCRs, such devices typically do not include a tuner, and are instead coupled to the satellite receiver or cable box. Also unlike VCRs, these devices are typically used to record digitized content, not analog video. This difference is both advantageous and disadvantageous.

20   An advantage of such devices is that they permit long term storage and multiple replays without substantial degradation. Another advantage is that they permit more rapid trick-play functions such as fast forwarding and rewinding. A disadvantage of such devices is that they are capable of making multiple-generation copies of the program material as well, and without serious degradation. This raises the very real possibility
25   that the multiple generation copies of the media programs will be produced and distributed without permission. This possibility has caused some media providers to be reluctant to allow their media programs to be recorded by such devices.

To ameliorate this problem, it is critical to protect the stored media programs with strong security and copy control. Current devices do not scramble media programs before
30   storage, nor do they store copy protection information. Instead, such devices record decrypted program content into the storage disk using a paired hardware scheme in which

the hard disk controller and hard disk are paired to each other specifically through a specific interface. Because the hard disk controller and the disk itself are essentially paired together, storage or playback will not function if the disk were to be removed and transferred to another player. The weakness of this security scheme is that it relies only

5   on the paired hardware to ensure security ... the media programs stored on the disk drive itself are not encrypted.

While it would presumably be possible to simply store the datastream as it is received from the broadcaster for later replay, this technique has distinct disadvantages. One such disadvantage is that it would provide pirates a permanently recorded version of

10 the encrypted datastream, thus providing the pirate with information that can be used to perform detailed analyses of the datastream itself to determine the encryption techniques and codes.

What is needed is a system and method for securely recording broadcast media programs (including impulse purchase pay-per-view programs) for limited use playback

15 at a later time. Such a system could be used to support video-on-demand (VOD), thus allowing the subscriber to purchase media programs and games from the set top box instantly without worrying about the start time of the program. What is also needed is a system and method that does not require substantial changes to subscriber hardware, such as the conditional access module (CAM) that is used to provide the key to decrypt the

20 media programs for presentation to the subscribers.

SUMMARY OF THE INVENTION

In summary, the present invention describes a system and method for storing and retrieving program material for subsequent replay. The method comprises the steps of

25 receiving access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key and control data; further encrypting the access control information and the encrypted program material according to a second encryption key; encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and storing the

30 encrypted access control information and encrypted program material and the fourth encryption key.

The apparatus comprises a tuner, for receiving encrypted access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key and control data; a first encryption module, communicatively coupled to the tuner and communicatively

5   coupleable to a data storage device, the first encryption module for further encrypting the encrypted program material and the access control information according to a second encryption key; a second encryption module, communicatively coupled to the first encryption module and communicatively coupleable to the data storage device, the second encryption module for encrypting the second encryption key according to a third

10   encryption key to produce a fourth encryption key; a first decryption module, communicatively coupleable to the disk drive, for decrypting the fourth encryption key to produce the second encryption key; a second decryption module, communicatively coupled to the first decryption module and the tuner and communicatively coupleable to the data storage device, for decrypting the further encrypted program material to produce

15   the encrypted program material and the encrypted access control information using the second encryption key; a conditional access module, communicatively coupleable to the second decryption module and the tuner, for selectably accepting the access control information selected from the group comprising the access control information received in the tuner and the access control information decrypted by the second decryption

20   module, the conditional access module comprising a third decryption module for decrypting the encrypted access control information to produce the first encryption key; and a fourth decryption module for decrypting the encrypted program material to produce unencrypted program material using the first encryption key.

One object of the present invention is to provide for the reception and decryption

25   of broadcast media programs, including impulse pay-per-view (IPPV) programs, that can be played and recorded onto storage media and allows playback at a later time with limited use. The data itself may be placed in short term storage, but the replay of the media programs can be accomplished with trick play functions such as forward, reverse, fast forward, fast reverse, frame advance, and pause functions.

30   Another object of the present invention is to provide PVR functions which provide recording, delayed playback, and trick play of IPPV media programs from the

storage media without requiring a pre-purchase of the IPPV media program. This would allow the IPPV media program to be purchased and viewed at the users leisure without requiring the IPPV media program to be purchased prior to storage. Ideally, such a system would allow the user to select the IPPV media program from the storage device,

5   subject to limited play rights.

Still another object of the present invention is to provide a pairing between the storage media and elements of the subscriber's IRD to assure that playback of the media programs from the storage device are permitted only with the proper IRD.

Still another object of the present invention is to provide a secure means for

10   storing broadcast data streams (including IPPV and games) on a data storage device, while providing for adequate copy protection.

Still another object of the present invention is to provide a system and method for handling the archiving and retrieving of media programs and other data, even if the data storage device fails.

15   Still another object of the present invention is to provide a system and method that allows media program purchases to be recorded in a way that is analogous to that which is employed for real-time off-the-air programs.

Still another object of the present invention is to provide a system that provides a growth path to a system permitting IPPV media programs to be previewed without charge

20   for an initial period of time with the option to purchase the media program or cancel the purchase, regardless of whether the program is retrieved from the storage device or obtained from a real time broadcast.

Still another object of the present invention is to achieve all of the foregoing without requiring substantial changes to conditional access module hardware and/or

25   software.

The present invention eliminates concerns regarding the proliferation of unauthorized digital copies of the media programs by use of a strong encryption method. Further, the present invention ensures that the stored material cannot be distributed since such decryption of the material can only be successfully performed by the encrypting

30   IRD.

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a diagram showing an overview of a video distribution system;

5   FIG. 2 is a block diagram showing a typical uplink configuration showing how video program material is uplinked to a satellite for transmission to subscribers using a single transponder;

FIG. 3A is a diagram of a representative data stream received from a satellite;

FIG. 3B is a diagram illustrating the structure of a data packet;

10   FIG. 4 is a block diagram illustrating a high-level block diagram of the IRD; and

FIGs. 5A-5C are diagrams illustrating the storage and retrieval of data from a media storage device.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

15   In the following description, reference is made to the accompanying drawings which form a part hereof, and which show, by way of illustration, several embodiments of the present invention. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

20

VIDEO DISTRIBUTION SYSTEM

FIG. 1 is a diagram illustrating an overview of a video distribution system 100. The video distribution system 100 comprises a control center 102 in communication with an uplink center 104 via a ground or other link 114 and an integrated receiver/decoder

25   (IRD) 132 at receiver station 130 via a public switched telephone network (PSTN) or other link 120. The control center 102 provides program material to the uplink center 104, coordinates with the receiver station 130 to offer subscribers 110 pay-per-view (PPV) program services, including billing and associated decryption of video programs.

The uplink center 104 receives program material and program control information

30   from the control center 102, and using an uplink antenna 106, transmits the program material and program control information to the satellite 108. The satellite 108 receives

and processes this information, and transmits the video programs and control information to the IRD 132 at the receiver station 130 via downlink 118. The IRD 132 receives this information using the subscriber antenna 112, to which it is communicatively coupled.

The video distribution system 100 can comprise a plurality of satellites 108 in

5 order to provide wider terrestrial coverage, to provide additional channels, or to provide additional bandwidth per channel. In one embodiment of the invention, each satellite comprises 16 transponders to receive and transmit program material and other control data from the uplink center 104 and provide it to the subscribers 110. However, using data compression and multiplexing techniques the channel capabilities are far greater. For

10 example, two-satellites 108 working together can receive and broadcast over 150 conventional (non-HDTV) audio and video channels via 32 transponders.

While the invention disclosed herein will be described with reference to a satellite based video distribution system 100, the present invention may also be practiced with terrestrial-based transmission of program information, whether by traditional

15 broadcasting means, cable, or other means. Further, the different functions collectively allocated among the control center 102 and the uplink center 104 as described above can be reallocated as desired without departing from the intended scope of the present invention.

Although the foregoing has been described with respect to an embodiment in

20 which the program material delivered to the subscriber is video (and audio) program material such as a movie, the foregoing method can be used to deliver program material comprising purely audio information or data as well.

FIG. 2 is a block diagram showing a typical uplink configuration for a single satellite 108 transponder, showing how video program material is uplinked to the satellite

25 108 by the control center 102 and the uplink center 104. FIG. 2 shows three video channels (which could be augmented respectively with one or more audio channels for high fidelity music, soundtrack information, or a secondary audio program for transmitting foreign languages), and a data channel from a computer data source 206.

The video channels are provided by a program source of video material 200A-

30 200C (collectively referred to hereinafter as video source(s) 200). The data from each video program source 200 is provided to an encoder 202A-202C (collectively referred to

hereinafter as encoder(s) 202). Each of the encoders accepts a presentation time stamp (PTS) from the controller 216. The PTS is a wrap-around binary time stamp that is used to assure that the video information is properly synchronized with the audio information after encoding and decoding. A PTS time stamp is sent with each I-frame of the MPEG

5   encoded data.

In one embodiment of the present invention, each encoder 202 is a second generation Motion Picture Experts Group (MPEG-2) encoder, but other decoders implementing other coding techniques can be used as well. The data channel can be subjected to a similar compression scheme by an encoder (not shown), but such

10   compression is usually either unnecessary, or performed by computer programs in the computer data source (for example, photographic data is typically compressed into *.TIF files or *.JPG files before transmission). After encoding by the encoders 202, the signals are converted into data packets by a packetizer 204A-204F (collectively referred to hereinafter as packetizer(s) 204) associated with each source 200, 206-210.

15   The data packets are assembled using a reference from the system clock 214 (SCR), a control word (CW) generated by the conditional access manager 208, and a system channel identifier (SCID) generator 210 that associates each of the data packets that are broadcast to the subscriber with a program channel. This information is transmitted to the packetizers 204 for use in generating the data packets. These data

20   packets are then multiplexed into serial data, encoded, modulated, and transmitted. A special packet known as a control word packet (CWP) which comprises control data including the control word (CW) and other control data used in support of providing conditional access to the program material is also encrypted and transmitted.

FIG. 3A is a diagram of a representative data stream. The first packet segment

25   302 comprises information from video channel 1 (data coming from, for example, the first video program source 200A). The next packet segment 304 comprises computer data information that was obtained, for example from the computer data source 206. The next packet segment 306 comprises information from video channel 5 (from one of the video program sources 200), and the next packet segment includes information from video

30   channel 1 (again, coming from the first video program source 200A). The data stream therefore comprises a series of packets from any one of the data sources in an order

determined by the controller 216. The data stream is encrypted by the encryption module 218, modulated by the modulator 220 (typically using a QPSK modulation scheme), and provided to the transmitter 222, which broadcasts the modulated data stream on a frequency bandwidth to the satellite via the antenna 106.

5   Subscribers 110 receive media programs via a subscriber receiver or IRD 132. Using the SCID, the IRD 132 reassembles the packets to regenerate the program material for each of the channels. As shown in FIG. 3A, null packets created by the null packet module 312 may be inserted into the data stream as desired.

FIG. 3B is a diagram of a data packet. Each data packet (e.g. 302-316) is 147

10   bytes long, and comprises a number of packet segments. The first packet segment 320 comprises two bytes of information containing the SCID and flags. The SCID is a unique 12-bit number that uniquely identifies the data packet's data channel. The flags include 4 bits that are used to control whether the packet is encrypted, and what key must be used to decrypt the packet. The second packet segment 322 is made up of a 4-bit packet type

15   indicator and a 4 -bit continuity counter. The packet type identifies the packet as one of the four data types (video, audio, data, or null). When combined with the SCID, the packet type determines how the data packet will be used. The continuity counter increments once for each packet type and SCID. The next packet segment 324 comprises 127 bytes of payload data, which is a portion of the video program provided by the video

20   program source 200. The final packet segment 326 is data required to perform forward error correction.

ENCRYPTION OF MEDIA PROGRAMS

Media programs are encrypted by the encryption module 218 before transmission

25   to assure that they are received and viewed only by authorized subscribers. Each media program is encrypted according to an alphanumeric encryption key referred to hereinafter as a control word (CW). This can be accomplished by a variety of data encryption techniques, including symmetric algorithms such as the data encryption standard (DES) and asymmetric algorithms such as the Rivest-Shamir-Adleman (RSA) algorithm.

30   To decrypt the media programs, the subscriber's 110 IRD 132 must also have access to the CW. To maintain security, CWs are not transmitted to the IRD 132

plaintext. Instead, CWs are encrypted before transmission to the subscriber's IRD 132. The encrypted CW is transmitted to the subscriber's IRD 132 in a control word (data) packet.

5   In one embodiment, the data in the CWP, including the CW, is encrypted and decrypted via what is referred to hereinafter as an input/output (I/O) indecipherable algorithm.

An I/O indecipherable algorithm is an algorithm that is applied to an input data stream to produce an output data stream. Although the input data stream uniquely determines the output data stream, the algorithm selected is such that it's characteristics

10   cannot be deciphered from a comparison of even a large number of input and output data streams. The security of this algorithm can be further increased by adding additional functional elements which are non-stationary (that is, they change as a function of time). When such an algorithm is provided with identical input streams, the output stream provided at a given point in time may be different than the output stream provided at

15   another time.

So long as the encryption module 218 and the IRD 132 share the same I/O indecipherable algorithm, the IRD 132 can decode the information in the CWP to retrieve the CW. Then, using the CW, the IRD 132 can decrypt the media program so that it can be presented to the subscriber 110.

20   To further discourage piracy, the control data needed to decrypt and assemble data packets into viewable media programs may be time-varying (the validity of the control data in a CWP to decode a particular media program changes with time). This can be implemented in a variety of ways.

For example, since each CWP is associated with a SCID for each media program,

25   the SCID related to each CWP could change over time.

Another way to implement time-varying control data is to associate time stamps with the received data stream and the CWP control data. In this case, successful decoding of the CWP to produce the CW would require the proper relationship between the time stamps for the data stream and the control data in the CWP. This relationship can be

30   defined, for example, by changing the decryption scheme used to generate the CW from the CWP according to the received time stamp for the data stream. In this case, if the

time stamp of the received data stream does not match the expected value, the wrong

decryption scheme will be selected and the proper CW (to decrypt the program material)

will not be produced. If, however, the time stamp of the received data stream matches the

expected value, the proper decryption scheme will be selected, and the CWP decryption

5   scheme will yield the proper CW.

REQUESTING PAY-PER-VIEW SERVICES

The data required to receive pay-per-view (PPV) media programs are stored in the

CWP and in another data packet known as the purchase information parcel (PIP). Both

10   the CWP and the PIP are broadcast to the subscriber via the video distribution system 100

in real time. As described below, the CWP is used by the IRD 132 to retrieve PPV media

programs.

Generally, PPV services can include operator-assisted pay-per-view (OPPV) and

impulse pay-per-view (IPPV) services. When requesting OPPV services, the subscriber

15   110 must decide in advance that they desire access to a particular media program. The

subscriber 110 then calls an entity such as the control center 102, and requests access to

the media program. When requesting impulse pay-per-view services (IPPV), the

subscriber 110, while viewing the program guide, moves the cursor over the viewer

channel associated with the desired media program, and selects "enter." After the

20   decision and rights to purchase a PPV program are confirmed (for example, by checking

channel lockouts, rating limits, and purchase limits), a purchase information parcel (PIP)

is received and stored in the subscriber's conditional access module 406 (which is

described in more detail below) for further use. The conditional access module 406

associates the information in the CWP and the PIP, and uses the PIP in conjunction with

25   the CWP to verify that the subscriber 110 should be provided access to the media

program and to decrypt the media program.

Ordering PPV media programs in advance using the PIP is limited, however, since

the PIP is broadcast up to 24 hours before the media program itself is broadcast. Since

the PIP is broadcast in real time, the IRD 132 does not acquire the PIP until the subscriber

30   110 actually requests the PPV media program purchase.

SUBSCRIBER RECEPTION AND DECRYPTION OF MEDIA PROGRAMS

FIG. 4 is a simplified block diagram of an IRD 132. The IRD 132 receives and decrypts the media programs broadcast by the video distribution system 100. These media programs are streamed to the IRD 132 in real time, and may include, for example,

5   video, audio, or data services.

The IRD 132 is communicatively coupleable to a conditional access module (CAM) 406. The CAM 406 is typically implemented in a smart card or similar device, which is provided to the subscriber 110 to be inserted into the IRD 132. The CAM 406 interfaces with a conditional access verifier (CAV) 408 which performs at least some of

10   the functions necessary to verify that the subscriber 110 is entitled to access the media programs. The CAV 408 is communicatively coupled to a metadata analysis module (MAM) 411. Using the information in metadata table (e.g. Table 1 described below), the MAM 411 acts as a gate-keeper to determine whether stored media programs will be decrypted and presented to the subscriber 110. This is accomplished by comparing the

15   metadata values with measured or accumulated values. The CAV 408 and the MAM 411 can be implemented as separate modules from the transport/demux/decryptor 412 and the microcontroller and memory 414 as shown, or may be implemented via software instructions stored in the memory and performed by the microcontroller 414. The functionality of the MAM 411 can also be implemented in the verifier 410 or in software

20   resident elsewhere in the IRD 132.

The IRD 132 comprises a tuner 410, a transport and demultiplexing module (TDM) 412, which operates under control of a microcontroller and associated memory 414, a source decoder 416 and communicatively coupled random access memory (RAM) 418, and a user I/O device for accepting subscriber 110 commands and for providing

25   output information to the subscriber.

The tuner receives the data packets from the video distribution system and provides the packets to the TDM 412. Using the SCIDs associated with each media program, the TDM 412 reassembles the data packets according to the channel selected by the subscriber 110, and unencrypts the media programs using the CW key. The TDM 412

30   can be implemented by a single secure chip, and is communicatively coupled to a microcontroller and memory 414.

Once the media programs are unencrypted, they are provided to the source decoder 416 which decodes the media program data according to MPEG or JPEG standards as appropriate. The decoded media program is then provided to a D/A converter (if necessary) and provided to external interfaces 404 which can include a

5 media program presentation device such as a television, an audio system, or a computer. The source decoder 416 makes use of communicatively coupled RAM 418 to perform these functions.

The CW key is obtained from the CWP using the CAV 408 and the CAM 406. The TDM 412 provides the CWP to the CAM 406 via the CAV 408. The CAM 406 uses

10 the I/O indecipherable algorithm to generate the CW, which is provided back to the TDM 412. The TDM 412 uses the CW to decrypt the media programs. In most IRDs 132, the CAV 408 and the CAM 406 are capable of decrypting one video/audio/data media program at a time.

As described above, to discourage potential pirates, the control data in the CWP

15 used to decode a particular media program may change with time so that it only produces the proper CW when applied to a media program having the proper time stamp. In this case, the CAM 406 can select and/or control the decryption scheme (e.g. the I/O indecipherable algorithm) according to the time stamp associated with the data stream carrying the media program. If the media program is sufficiently disassociated in time,

20 the improper decryption scheme will be used, and the proper CW to decode the media program will not be produced.

Further details regarding the encryption and decryption of media programs can be found in co-pending and commonly assigned U.S. Patent Application Serial No. 09/491,959.

25

STORAGE AND RETRIEVAL OF MEDIA PROGRAMS IN ENCRYPTED FORM

FIG. 5A is a diagram presenting exemplary method steps used to practice one embodiment of the present invention. A data stream 501 is provided by the subscriber antenna 112 and received by the tuner 410 and the TDM 412, as shown in block 502. The

30 data stream 501 includes a plurality of data packets including data packets with the program material encrypted according to a first encryption key (CW key 546 as seen in

FIG. 5B), and one or more control word packets (CWP) 504. The control word packets 504 contain access control information and other data which may be processed to produce the CW key 546 necessary to decrypt the program material.

The data stream 501 may also include metadata describing information including rights associated with the program material (which may include, for example, replay rights and/or copy rights). These rights include parameters necessary for controlling the replay of program material, including IPPV or pay-per-play services. The metadata can include information as described in Table I below:

Right	Value	Comment
Storage	N_0	N_0 index indicates whether the program material is permitted to be stored long-term on the media storage device 528 (value 1) or if it was intended for real time viewing only (value 0).
Lifetime without purchase	N_1	N_1 index indicates how long an item is permitted to be stored onto the media storage device 528 without actually being purchased. This time period could be days, weeks or months depending on the business case. When/if this time limit is reached, the associated program material is erased from the media storage device 528.
Lifetime after purchase	N_2	N_2 index indicates how long program material is permitted to be stored onto the hard disk after being purchased. This time period could be days, weeks or months depending on the business case. When/if this time limit is reached, the associated program

Right	Value	Comment
		is erased from the media storage device 528.
Views per pay	N_3	N_3 index indicates how many times a subscriber is permitted to use/view the program material per times it was paid for. For example, a value of 0 could indicate unlimited use, and any non-zero value could indicate how may uses are allowed per pay.
Repurchase a program	N_4	N_4 indicates the cost associated with repurchasing a program after the N_3 value has been exceeded (assuming N_3 is not unlimited). Depending on the business case, N_4 may or may not be higher or lower than the original purchase offer price.
Views per repurchase	N_5	N_5 would indicate how many times a user would be able to use/view the program material after it had been purchased once. For example, a value of 0 could indicate unlimited use, and any non-zero value could indicate how may uses are allowed per pay. Depending on the business case, the value for N_5 may or may not be the same as N_3.
Reserved	N_6 - N_M	Reserved values to place additional limits on the usage of downloaded materials. The value of M could be as large or as small as needed depending on the complexity of the desired business case.

Table I

If the program material is not to be stored in the media program storage device 528 (as indicated by the switch controlled by N_0), the encrypted program material 506 and the CWP 504 are processed normally, as shown in FIG. 5B. The CWP 504 is presented to the IPPV control module in the CAM 406 which analyzes the access control information

5 in the CWP 504 to determine whether or not the subscriber is entitled to view the program material. If so, the CW extraction module 544 produces the control word from data in the CWP and supplies it to the broadcast decrypt module 510 to decrypt the program material 511 for display.

The information describing the subscriber's rights to view the program material

10 (e.g. Table I) may have been previously received from the service provider or from an IPPV purchase action or a subscriber-initiated action preceding the viewing of the program. The subscriber action commands the IPPV control module 540 in the CAM 406 to store IPPV entitlement information in the purchase history module 542 in the CAM 406 for later reporting to the service provider.

15 In one embodiment, the metadata table is initially provided to the subscriber with defaults for each of the settings, and/or is supplied as a part of the IRD 132 software. When a program is broadcast that is to be stored onto the hard disk for storage and later PPV, the default metadata table is attached (e.g. by the IRD 132 verifier 408). For the majority of the broadcasted events and programs, the default settings are sufficient, and

20 no further changes are required.

If a need arises to change one of the settings for a particular program, the change to the specific parameter, and not the entire metadata table, is broadcast to the subscriber. The IRD 132 then recognizes the parameter change, and modifies the metadata table according to the specific parameter change. This way, the broadcaster is required only to

25 broadcast the non-default values, and not the same table for each program. This saves valuable broadcast bandwidth and IRD 132 operations required to build and store multiple metadata tables.

The metadata could also be used to pre-cache content onto a subscriber's 110 storage device 528. The content would be "hidden" from the subscriber 110 until a

30 specified time and/or date, or another condition (which can be described in the metadata table) takes place. For example, the program title would not initially be presented in the

available cache or other areas of the user interface. After the appropriate condition is satisfied (e.g. at the appropriate time), the content would then be presented to the subscriber 110 as an available program. This would allow the video broadcast system to send content at opportune times for broadcast, such as during the night when bandwidth

5   demands are low. This can happen either the day of an event or even weeks ahead of time. These pre-cached events could be triggered to present content that relates to either special events or during times and dates specified by the content providers.

The metadata can also be provided as a part of the data stream 501 from a different satellite 108 transponder than the program material, from a different satellite

10   108, or from a land link such as the PSTN link 120.

After suitable processing (i.e. MPEG and or JPEG decoding, decompression, conversion to an analog signal, etc.), the program material 511 is provided to an external interface 404 device, which may include a presentation device such as a display 548.

If the program material is to be stored in the media program device 528, the

15   encrypted program material 506 (denoted Encrypted V/A/D in FIGs. 5A-5C to indicate that the program material can include video, audio, or other data) is provided to a storage encryption module 512. The storage encryption module 512 further encrypts the encrypted program material 506 and the CWP 504 according to a CP encryption key 516. Further, a key encryption module 522 encrypts the CP key 516 with a box key 520 to

20   produce an encrypted CP key 524. The resulting further encrypted program material 514, the encrypted CWP 518, and the encrypted CP key 524 are stored in the media storage device 528. When replay of the stored program material is desired, the further encrypted program material 514, the encrypted CWP 518 and the encrypted CP key 524 are retrieved from the media storage device 528 as depicted in block 530. Using the box key

25   520, the encrypted CP key 524 is decrypted by the key decryption module 532 to produce the CP key 516. The CP key 516, the further encrypted program material 514 and the encrypted CWP 518 is provided to the storage decrypt module 534. Using the CP key 516, the CP decrypt module 534 produces the encrypted program material 506 (still encrypted with the CW key as it was when it was received by the tuner 410) and the CWP

30   504 (which is again in the same form as it was when it was received by the tuner 410).

Should the storage device 528 fail, the data stored therein may still be recovered. Unlike prior art video storage devices, which prevent copying of the data from the storage media via a controller that writes data to the storage media, the present invention stores the data in encrypted form as well as at least part of the information required

5   Since the present invention stores data in encrypted form as well as a key required to decrypt the data (using other keys in the IRD 132), the present invention allows the user to back up data stored in the media storage device 528 on another data storage device such as a zip drive or a writable CD ROM. Further, the such backup data is encrypted, and not exposed to copying.

10   FIG. 5B is a diagram showing additional operations performed when the subscriber 110 elects to view program material stored on the media storage device 528.

     When the subscriber 110 elects to view recorded program material, the MAM 411 compares the metadata associated with the program material (which may include data regarding the rights shown in Table I above) with other stored information to determine

15   whether the recorded program material should be decrypted and presented. If the comparisons performed by the MAM 411 indicate that the stored program material should be decrypted and presented to the subscriber 110, the CWP 504 is provided to the CAM 406. The CAM 406 includes an IPPV (impulse pay-per-view) control module 540 which commands CW extraction module 544 to decrypt the CWP 504 to produce the CW

20   546, and provides information regarding the subscriber's 110 decision to purchase the right to view the program material to a purchase history module 542. The purchase history module 542 records information regarding the subscriber's 110 purchase, and provides the information to the entity that provided the program material to the subscriber for billing purposes. The IPPV control module 540 essentially performs the same

25   functions as that which would be required for non-storage compatible operations. Hence, the foregoing functionality is accomplished without resort to changes in CAM 406 functionality.

     Importantly, the embodiment described above does not require changes to the CAM 406, since the operations described in FIG. 5B are exactly the same as normal

30   operation when the program material is not stored on the media storage device. Further, this embodiment does not require alteration of the CWP 504 to account for any

temporally varying relationship between the information in the CWP 504 and the program material. That is because any time-dependent relationship between the SCIDs of the program material and the CWP are preserved when they are encrypted and stored on the media storage device.

5   FIG. 5C is a diagram showing an embodiment of the present invention in which the unencrypted program material is re-encrypted and stored on the data storage device 528 (or a second data storage device separate from the data storage device 528) and retrieved for presentation to the subscriber 110. This embodiment is useful, for example, to support the enforcement of the replay and copy protection rights described in Table I.

10   This embodiment is also useful when the subscriber 110 requests trick play operations in viewing program material stored on the media storage device 528. These trick play operations include, for example, a play command; a rewind command; a fast forward command; a fast reverse play command; a fast forward play command; a pause command; a frame step command; and a stop command.

15   In this embodiment, the unencrypted program material 511 is not provided directly for display, but rather copy protection encrypted, stored in the data storage device 528 (or a second data storage device), and retrieved and decrypted before providing the program material for display. In particular, the unencrypted program material 511 is provided to a second Storage Encrypt Module 550. The second Storage Encrypt Module

20   550 encrypts the unencrypted program material 511 using the CP encryption key 516 to produce re-encrypted program material 552. The CP encryption key 516 is also encrypted by the key encrypt module 522 to produce the encrypted CP key 524. Both the re-encrypted program material 552 and the encrypted CP key 524 are stored in the media storage device 528.

25   When a user command is provided to the user I/O 420 that requires playback of the program material, the re-encrypted program material 552 and encrypted CP key 524 are retrieved from the media storage device 528. The encrypted CP key is decrypted by the key decrypt module 532 to produce the CP encryption key 516. The re-encrypted program material 552 and the CP encryption key 516 is provided to a storage decrypt

30   module 554. The storage decrypt module 554 decrypts the re-encrypted program material

552 to produce a clear version of the program material 511. The program material 511 is provided to an external interface 404 such as the display 548 for presentation to the user.

In the preferred embodiment, the storage encrypt module 550 and decrypt modules 554 described above with respect to FIG. 5C are different modules than that which are described and illustrated in FIG. 5A. This allows parallel encryption operations to be performed, thus speeding up the process, and allowing for the application of different CP encryption keys. However, the present invention may also be implemented such that the same CP encrypt and decrypt modules are used for both operations. This includes an implementation where different CP keys are used, and switched into the modules as required.

Similarly, it should be noted that FIGs. 5A and 5C illustrate an embodiment wherein the storage encrypt and storage decrypt modules 550, 554 are separate modules. However, the present invention may also be implemented with a single Storage Encryption and Decryption module, which may be switched between encrypt and decrypt functionality.

Similarly, the key encrypt and decrypt functionality described in FIGs. 5A and 5C are illustrated as separate modules, whereas the same optional usage of one or more modules may be utilized to perform the functionality.

The present invention also envisions the use of the same or similar encryption mechanisms are used for the broadcast decryption, storage encryption and decryption, and key encryption and decryption to allow one or more such modules to perform any of the encrypt or decrypt functions described in FIGs. 5A and 5C.

Generally, the box key 520 is unique to the IRD 132 and the CP key is unique to the media program, but this need not be the case. Further, different techniques and mechanisms can be used to generate and install the IRD-unique box key 520 and the media program unique CP key. In a preferred embodiment, the box key 520 is factory configured, and the CP key is generated randomly by the IRD 132, and is unique for each stored media program.

Finally, it is noted that in the embodiment described above, the media storage device 528 depicted in FIG. 5C is the same media storage device 528 depicted in FIG. 5A. If desired, however, the re-encrypted program material 552 can be stored in a second

(and separate) media storage device. For that matter, any of data described in the foregoing can be stored in a plurality of media storage devices to increase throughput or facilitate additional security measures. This embodiment would permit faster storage and retrieval of information from the disk(s).

5   In the foregoing embodiment of the present invention, the data stream received in IRD 132 further includes metadata including data to control replay rights and copy protection. This metadata is stored in the media storage device 528 for later use when a request to view the media program is received. The stored metadata may or may not be encrypted and/or signed.

10

Conclusion

The present invention describes a system and method for recording program related material that has not yet been purchased, and allow IPPV purchase at the time of replay and viewing. Billing will only be applied if the purchase is made. The data stream 15   501 having the program material is subject to different limitations on such storage and replay depending on the associated metadata for each program. The program material can be presented to the subscriber 110 in real time, or can be further encrypted prior to storage for later playback. In either case, program material is not stored plaintext. Caching techniques can be used to allow the user to delay or shift a program, or to support trick 20   play functions.

When the program material and associated data is not intended to be stored on the hard disk for later playback, the IRD 132 sends the encrypted program material 506 and associated CWP 504 to the CAM 406. The CAM 406 decrypts the CWP 504 to obtain the CW key 546, and the CW key 546 is used to decrypt the program material so that it 25   can be presented to the subscriber 110.

If a media storage device 528 is available to the IRD 132, the media program can be decrypted, re-encrypted, and stored in the media storage device as a cache to allow the user to pause, rewind, fast forward or any other functions that might be incorporated as part of trick play functions.

30   If a media storage device 528 is available to the IRD 132 and the data is to be stored on the hard disk prior to purchase for later purchase and playback, the IRD 132

bypasses CAM 406 processing and sends the encrypted program material 506 and associated CWP 504 directly to an encryptor engine 512 (typically included within the transport chip). and bypass being processed by the CAM. Once the data is further encrypted, the information is stored.

5   The present invention uses metadata associated with each media program that is included in the broadcast data stream. The metadata includes information describing the rights available to the subscriber 110 in terms of viewing and/or copying the program material. The "rights" associated with the program material could be presented to the subscriber 110 in a user-friendly manner.

10   The "rights" described in the metadata may allow the subscriber to view a media program an unlimited number of times within a time period (video store model); a set number of times within a time period (modified video store model); allow the user only one play within a set time period (movie theater model); and allow different pricing models for the different views (i.e. pay 1X for the first usage, ½ X for second viewing, 15   etc.). Other models would allow storage of media programs for set availability windows and then automatically delete the programs after the availability window is closed. Because the access control information as well as the associated program material, the present invention can be effectively utilized in systems in which the access control information is time-varying.

20   Typically, the IRD 132 handles the generation, encryption, and decryption of the encryption keys. The IRD 132 also includes the necessary hardware and software to install and restore keys for copy protected service.

While the foregoing description has focused primarily on the storage and retrieval of video programs, the present invention is not limited to these media types. As such, the 25   terms "media program" or "program material" describe a video data stream, and/or an audio data stream, and/or any other broadcast data stream, regardless of the data type.

The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications 30   and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims

CLAIMS

What is Claimed is:

1. A method of storing program material for subsequent replay, comprising the steps of:

receiving access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key and control data;

further encrypting the access control information and the encrypted program material according to a second encryption key;

encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

storing the encrypted access control information and encrypted program material and the fourth encryption key.

2. The method of claim 1, further comprising the steps of:

reading the further encrypted access control information and encrypted program material and the fourth encryption key;

decrypting the further encrypted access control information to produce the encrypted access control information;

decrypting the fourth encryption key using the third encryption key to produce the second encryption key;

decrypting the encrypted access control information to produce the first encryption key; and

decrypting the program material using the first encryption key.

1   3.   The method of claim 2, wherein

2   the access control information further comprises data describing a right associated

3 with the program material; and

4   the steps of decrypting the encrypted access control information to produce the

5 first encryption key and decrypting the program material using the first encryption key is

6 performed according to the data describing the right.

1   4.   The method of claim 3, wherein the right is expressed in a metadata table.

1   5.   The method of claim 4, wherein the metadata table comprises data selected

2 from the group comprising:

3   at least one default value wherein the data describing a right associated with the

4 program material comprises a change to at least one of the default values; and

5   at least one control value expressing a condition that must be satisfied before pre-

6 cached program material is presented to the subscriber.

1   6.   The method of claim 3, wherein the right is selected from the group

2 comprising:

3   a storage right;

4   a viewing right, having at least one viewing right characteristic selected from the

5 group comprising:

6   a non-purchase lifetime of the program material;

7   a lifetime of the program material after a purchase of the program material;

8   a number of permitted views per purchase of the program material;

9   a cost to repurchase the program material; and

10 a number of permitted views per repurchase of the program material.

1   7.   The method of claim 2, further comprising the step of providing the

2 decrypted program material to a presentation device.

1   8.   The method of claim 2, further comprising the steps of:

2   storing the decrypted program material; and

3   reading the decrypted program material according to a user command.

1   9.   The method of claim 8, wherein the user command is selected from the

2 group comprising:

3   a play command;

4   a rewind command;

5   a fast forward command;

6   a fast reverse play command;

7   a fast forward play command;

8   a pause command;

9   a frame step command; and

10   a stop command.

1   10.   The method of claim 2, further comprising the steps of:

2   re-encrypting the decrypted program material according to the second encryption

3 key;

4   encrypting the second encryption key according to a third encryption key to

5 produce a fourth encryption key; and

6   storing the re-encrypted program material and the fourth encryption key.

1   11.   The method of claim 10, wherein:

2   the access control information further comprises data describing viewing rights for

3 the program material; and

4   the steps of decrypting the encrypted access control information to produce the

5 first encryption key and decrypting the program material using the first encryption key is

6 performed according to the data describing the viewing rights.

1   12.   The method of claim 11, further comprising the steps of:

2   reading the re-encrypted program material and the fourth encryption key;

3   decrypting the fourth encryption key with the third key to produce the second

4 encryption key; and

5   decrypting the program material using the second encryption key.

1   13.   The method of claim 12, further comprising the step of providing the

2 decrypted program material to a presentation device.

1   14.   The method of claim 12, wherein the steps of reading the re-encrypted

2 program material and the fourth encryption key, decrypting the fourth encryption key

3 with the third encryption key to produce the second encryption key, and decrypting the

4 program material using the second encryption key are performed according to a user

5 command.

1   15.   The method of claim 14, wherein the user command is selected from the

2 group comprising:

3   a play command;

4   a rewind command;

5   a fast forward command;

6   a fast reverse play command;

7   a fast forward play command;

8   a pause command;

9   a frame step command; and

10   a stop command.

1   16.   An apparatus for storing program material for subsequent replay,

2 comprising:

3   a tuner, for receiving encrypted access control information and the program

4 material encrypted according to a first encryption key, the access control information

5 including the first encryption key and control data;

6   a first encryption module, communicatively coupled to the tuner and

7 communicatively coupleable to a data storage device, the first encryption module for

8 further encrypting the encrypted program material and the access control information

9 according to a second encryption key;

10   a second encryption module, communicatively coupled to the first encryption

11 module and communicatively coupleable to the data storage device, the second

12 encryption module for encrypting the second encryption key according to a third

13 encryption key to produce a fourth encryption key;

14   a first decryption module, communicatively coupleable to the disk drive, for

15 decrypting the fourth encryption key to produce the second encryption key;

16   a second decryption module, communicatively coupled to the first decryption

17 module and the tuner and communicatively coupleable to the data storage device, for

18 decrypting the further encrypted program material to produce the encrypted program

19 material and the encrypted access control information using the second encryption key;

20   a conditional access module, communicatively coupleable to the second

21 decryption module and the tuner, for selectably accepting the access control information

22 selected from the group comprising the access control information received in the tuner

23 and the access control information decrypted by the second decryption module, the

24 conditional access module comprising a third decryption module for decrypting the

25 encrypted access control information to produce the first encryption key; and

26   a fourth decryption module for decrypting the encrypted program material to

27 produce unencrypted program material using the first encryption key.

1   17.   The apparatus of claim 16, further comprising:

2   a third encryption module, communicatively coupled to the fourth decryption

3   module and communicatively coupleable to a second media storage device, the third

4   encryption module for encrypting the unencrypted program material according to the

5   second encryption key; and

6   a fifth decryption module, communicatively coupleable to the second media

7   storage device, for decrypting the encrypted program material using the second

8   encryption key.

1   18.   The apparatus of claim 17, wherein the third encryption module encrypts

2   the unencrypted program material and provides the encrypted program material to the

3   data storage device when a subscriber selects a trick play operation

1   19.   The apparatus of claim 17, wherein the third encryption module encrypts

2   the unencrypted program material and provides the encrypted program material to the

3   data storage device when the subscriber purchases the program material.

1   20.   The apparatus of claim 16, wherein:

2   the fourth decryption module is communicatively coupled to the first encryption

3   module; and

4   the second decryption module is communicatively coupleable to a presentation

5   device.

1   21.   The apparatus of claim 20, wherein:

2   the first encryption module encrypts the unencrypted program material using the

3   second encryption key, and provides the encrypted program material to the data storage

4   device; and

5   the second decryption module accepts the encrypted program material from the

6   data storage device and decrypts the encrypted program material using the second

7   encryption key.

1   22.   The apparatus of claim 16, further comprising the data storage device, for

2   storing and retrieving the further encrypted program materials and the fourth encryption

3   key.

1   23.   The apparatus of claim 16, wherein the third decryption module is

2   implemented in a smartcard.

1   24.   The apparatus of claim 16, wherein the control data is temporally variant.

1   25.   An apparatus for storing program material for subsequent replay,

2   comprising:

3   means for receiving access control information and the program material

4   encrypted according to a first encryption key, the access control information including the

5   first encryption key and control data;

6   means for further encrypting the access control information and the encrypted

7   program material according to a second encryption key;

8   means for encrypting the second encryption key according to a third encryption

9   key to produce a fourth encryption key; and

10   means for storing the encrypted access control information and encrypted program

11   material and the fourth encryption key.

26.   The apparatus of claim 25, further comprising:

means for retrieving the further encrypted access control information and encrypted program material and the fourth encryption key;

means for decrypting the further encrypted access control information to produce the encrypted access control information;

means for decrypting the fourth encryption key using the third encryption key to produce the second encryption key;

means for decrypting the encrypted access control information to produce the first encryption key; and

means for decrypting the program material using the first encryption key.

27.   The apparatus of claim 26, wherein:

the access control information further comprises data describing at least one right for the program material; and

encrypted access control information the encrypted program material is decrypted according to the data describing the right.

28.   The apparatus of claim 27, wherein the right is selected from the group comprising:

a storage right;

a viewing right, having at least one viewing right characteristic selected from the group comprising:

a non-purchase lifetime of the program material;

a lifetime of the program material after a purchase of the program material;

a number of permitted views per purchase of the program material;

a cost to repurchase the program material; and

a number of permitted views per repurchase of the program material.

29.   The apparatus of claim 26, further comprising means for providing the decrypted program material to a presentation device.

1   30.   The apparatus of claim 26, further comprising:

2   means for storing the decrypted program material; and

3   means for retrieving the decrypted program material according to a user

4   command.

1   31.   The apparatus of claim 30, wherein the user command is selected from the

2   group comprising:

3   a play command;

4   a rewind command;

5   a fast forward command;

6   a fast reverse play command;

7   a fast forward play command;

8   a pause command;

9   a frame step command; and

10   a stop command.

1   32.   The apparatus of claim 26, further comprising:

2   means for re-encrypting the decrypted program material according to the second

3   encryption key;

4   means for encrypting the second encryption key according to a third encryption

5   key to produce a fourth encryption key; and

6   means for storing the re-encrypted program material and the fourth encryption

7   key.

1   33.   The apparatus of claim 32, wherein:

2   the access control information further comprises data describing at least one right

3   for the program material; and

4   encrypted access control information the encrypted program material is decrypted

5   according to the data describing the right.

1   34.   The apparatus of claim 33, further comprising:

2   means for reading the re-encrypted program material and the fourth encryption

3 key;

4   means for decrypting the fourth encryption key with the third key to produce the

5 second encryption key; and

6   means for decrypting the program material using the second encryption key.

1   35.   The apparatus of claim 34, further comprising means for providing the

2 decrypted program material to a presentation device.

1   36.   The apparatus of claim 34, wherein the re-encrypted program material and

2 the fourth encryption key is read, the fourth decryption key is decrypted with the third key

3 to produce the second encryption key, and the program material is decrypted using the

4 second decryption key according to a user command.

1   37.   The apparatus of claim 36, wherein the user command is selected from the

2 group comprising:

3   a play command;

4   a rewind command;

5   a fast forward command;

6   a fast reverse play command;

7   a fast forward play command;

8   a pause command;

9   a frame step command; and

10   a stop command.

VIDEO ON DEMAND PAY PER VIEW SERVICES WITH UNMODIFIED CONDITIONAL ACCESS FUNCTIONALITY

ABSTRACT OF THE DISCLOSURE

5   A system and method for storing and retrieving program material for subsequent replay is disclosed. The method comprises the steps of receiving access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key and control data; further encrypting the access control information and the encrypted program material according to a second encryption key; encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and storing the encrypted access control information and encrypted program material and the fourth encryption key.
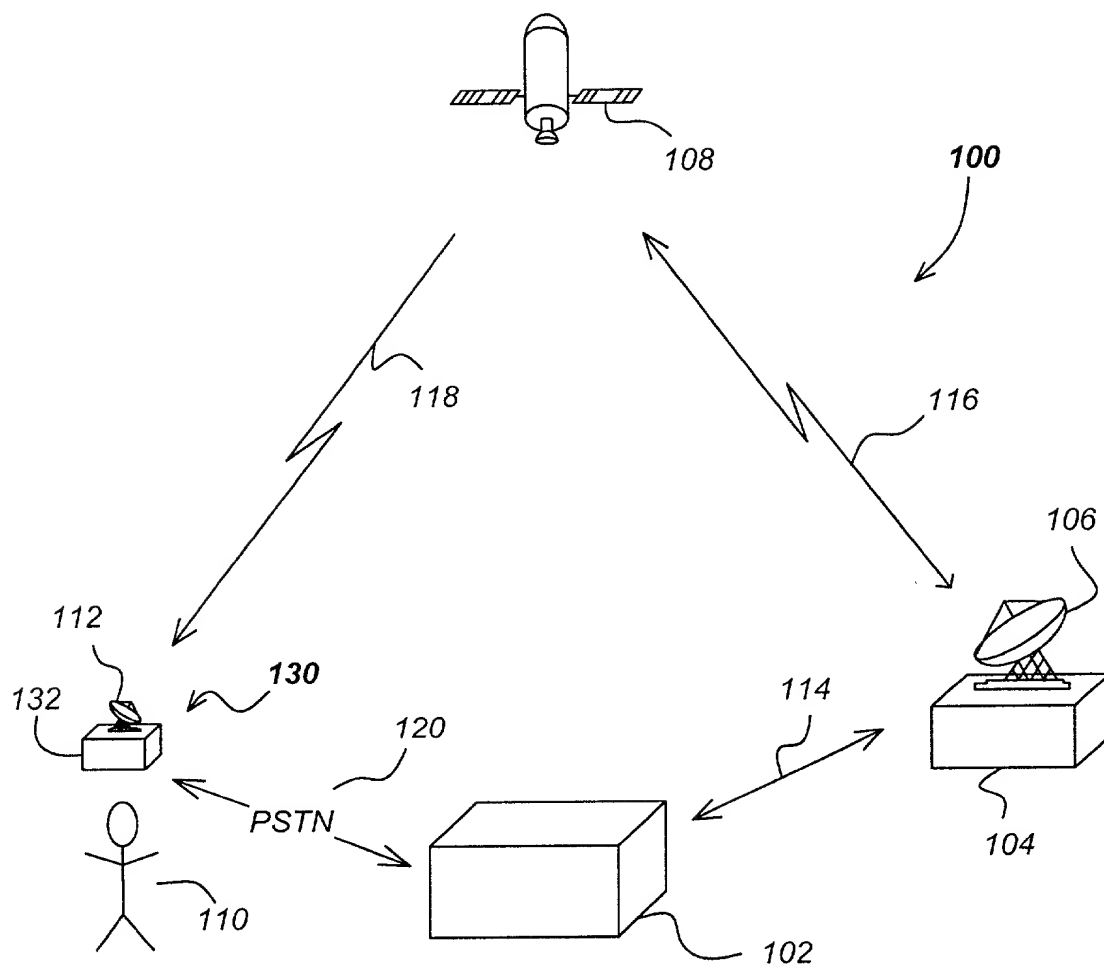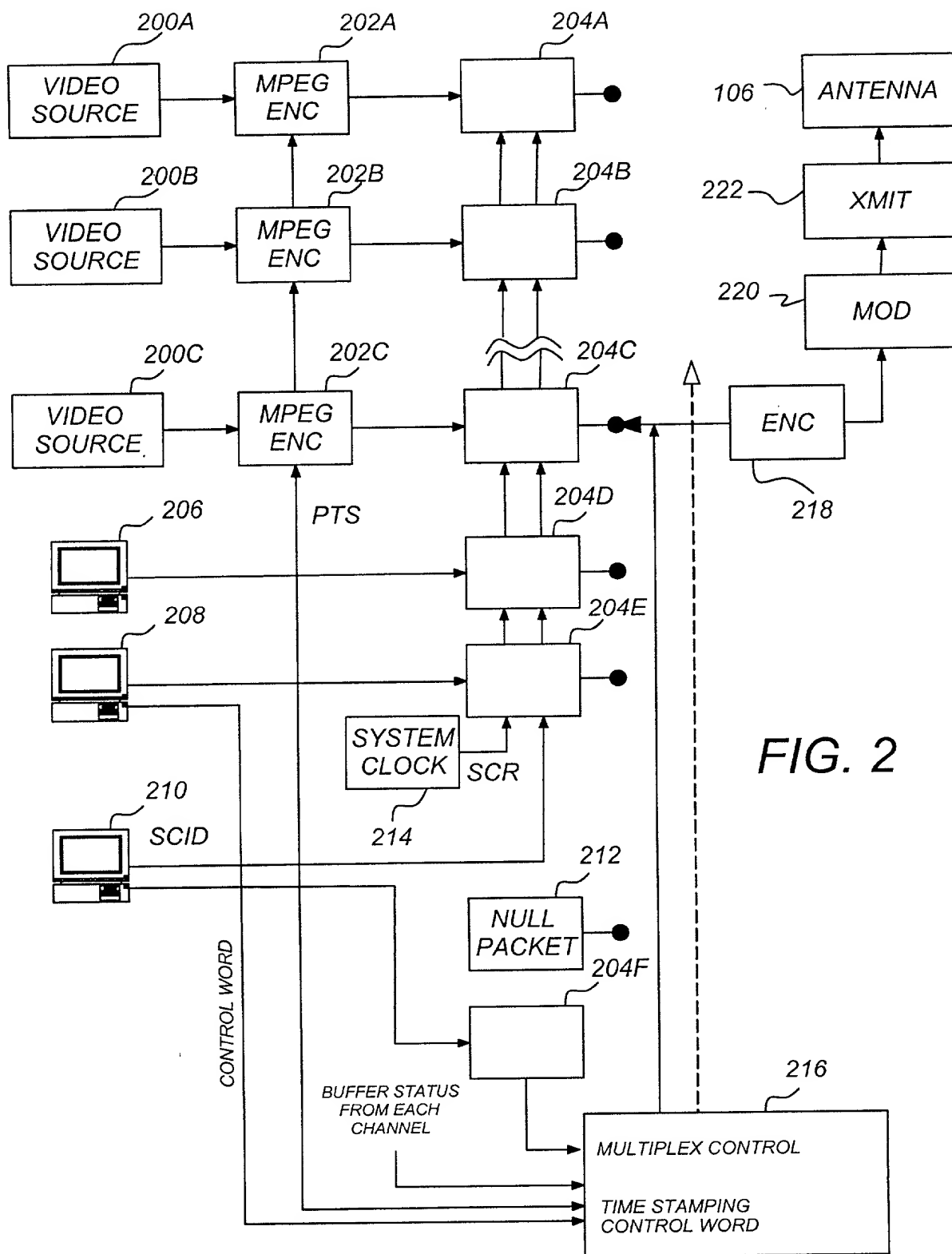
108

100

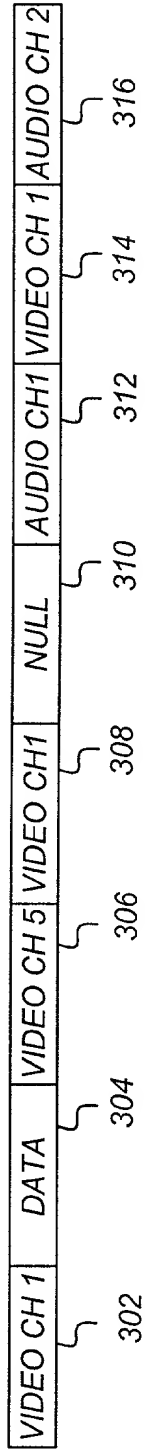**118**

116

112

106

132

130

120

114

PSTN

110

104

102

FIG. 1

FIG. 2

VIDEO CH 1	DATA	VIDEO CH 5	VIDEO CH1	NULL	AUDIO CH1	VIDEO CH 1	AUDIO CH 2
302	304	306	308	310	312	314	316

FIG. 3A

SCID & FLAGS 320	PACKET TYPE & CONTINUITY COUNTER 322	PAYLOAD	FEC
		324	326

FIG. 3B

FIG. 4

CAM
406

132

MICROCONTROLLER
AND
MEMORY
414

USER I/O
420

CA
VERIFIER
408

METADATA
ANALYSIS
MODULE
411

TRANSPORT/
DEMUX/DECRYPT
412

SOURCE
DECODING
VIDEO/AUDIO
DATA
416

RAM
418

EXTERNAL
INTERFACES
404

TUNER
410

FIG. 5A

FIG. 5B

STORE
554

528

Re-encrypted V/A/D
552

550

STORAGE ENCRYPT MODULE
511

Clear V/A/D

BROADCAST DECRYPT MODULE
506

510

Encrypted V/A/D

a

b

MAM
411

CWP

504
CAM

IPPV CONTROL MODULE
540

PURCHASE HISTORY MODULE
542

CW EXTRACTION MODULE
544

CW 546

406

KEY ENCRYPT MODULE
522

CP KEY 516
c

BOX KEY 520
d

ENCRYPTED CP KEY 524

KEY DECRYPT MODULE
532

CP KEY 516

Re-encrypted V/A/D
552

STORAGE DECRYPT MODULE
554

511

Clear V/A/D

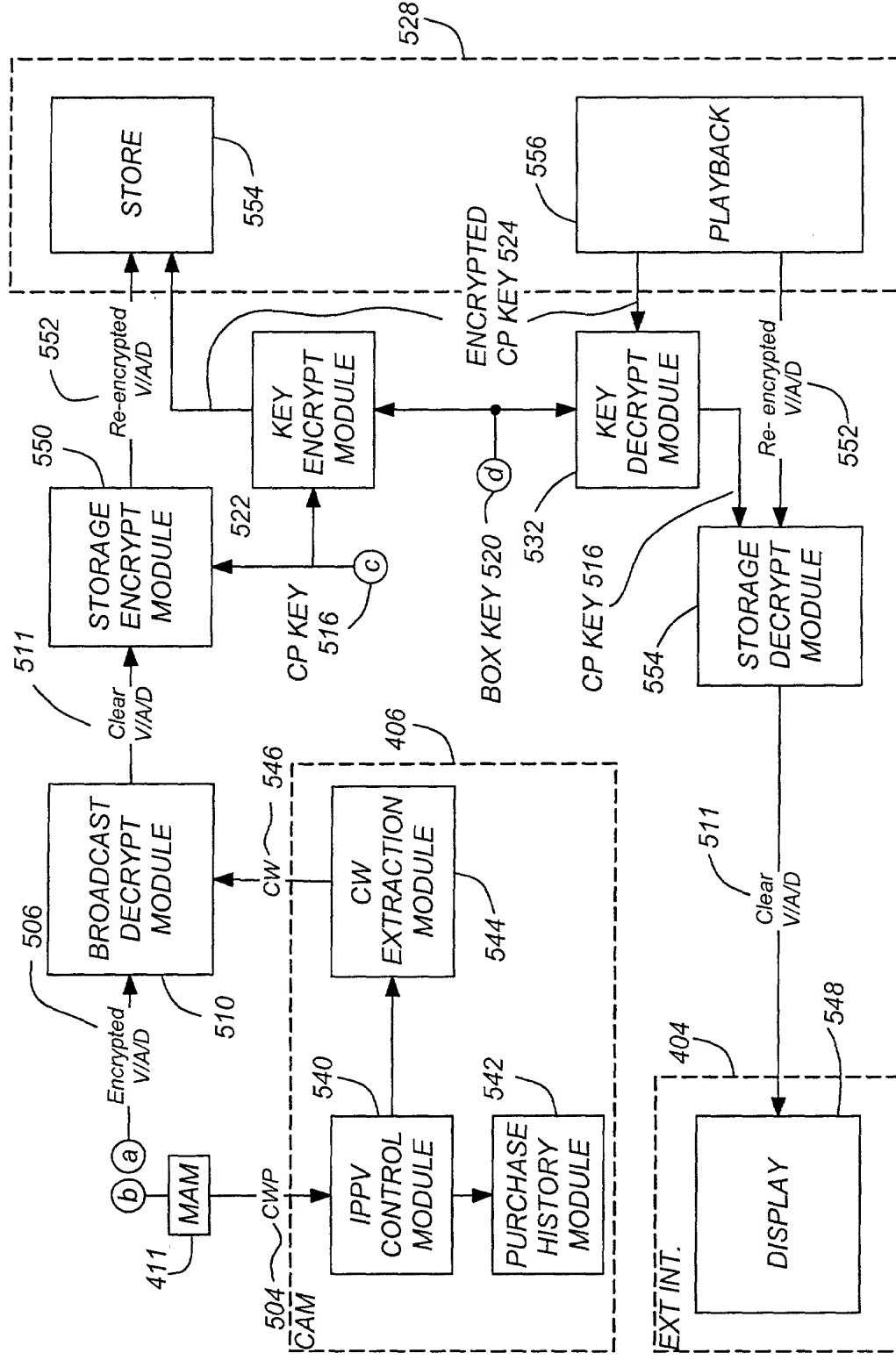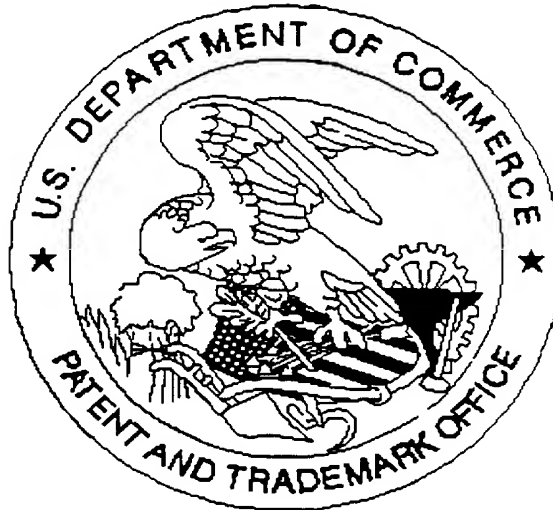DISPLAY
548

404
EXT INT.

PLAYBACK
556
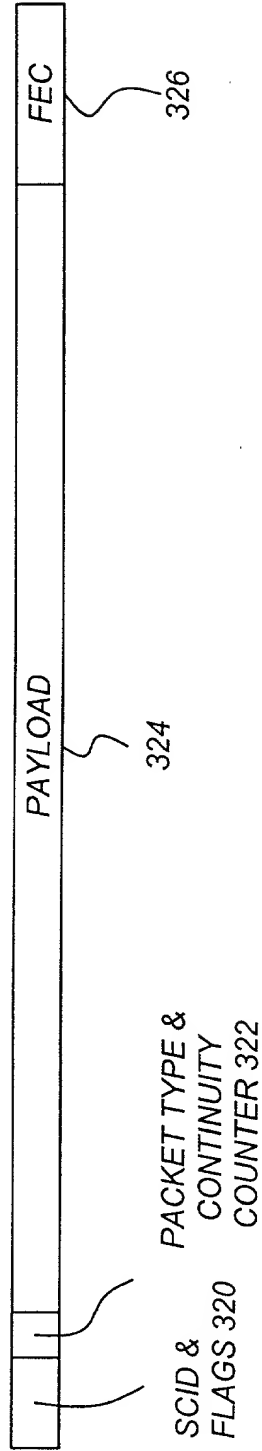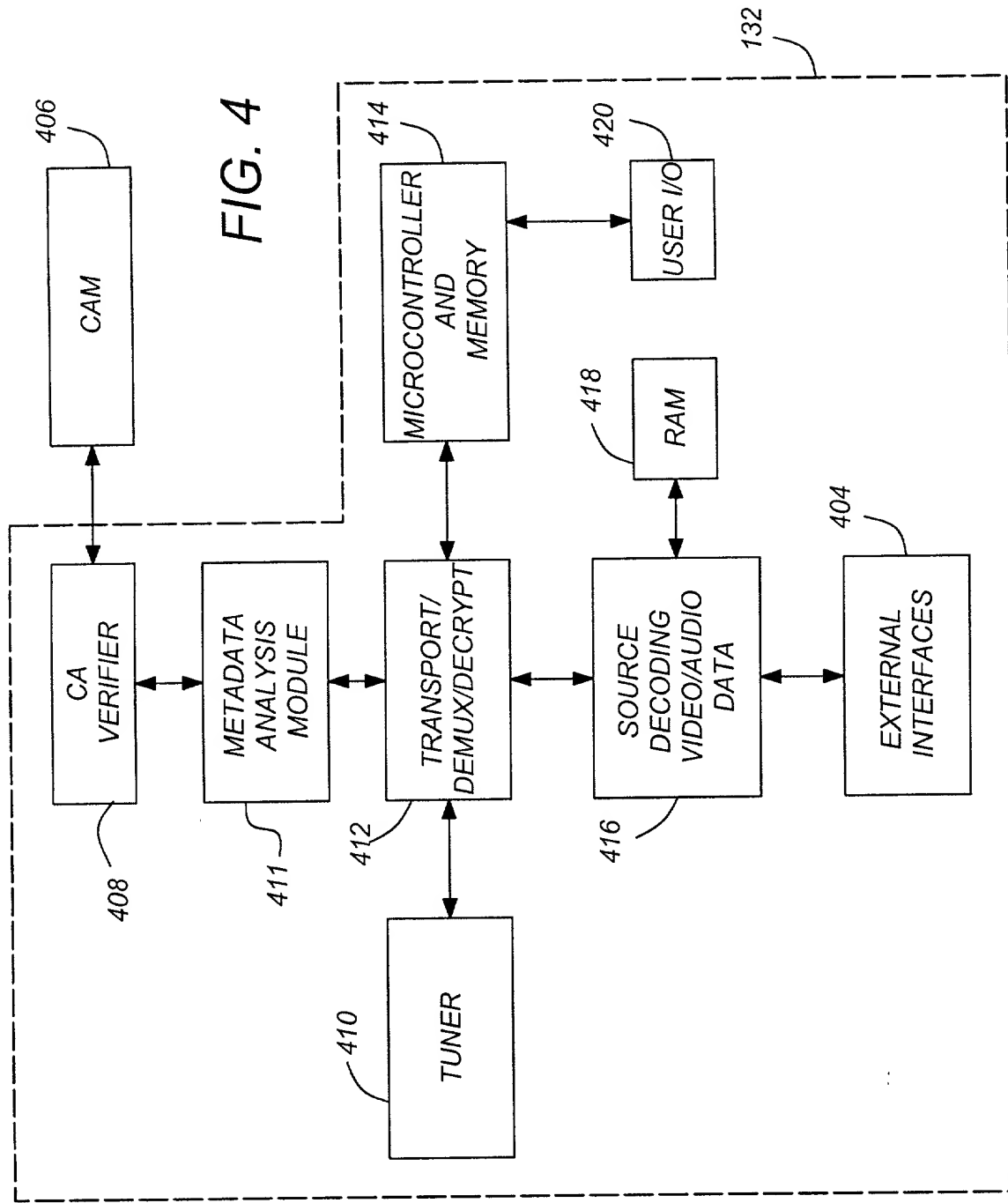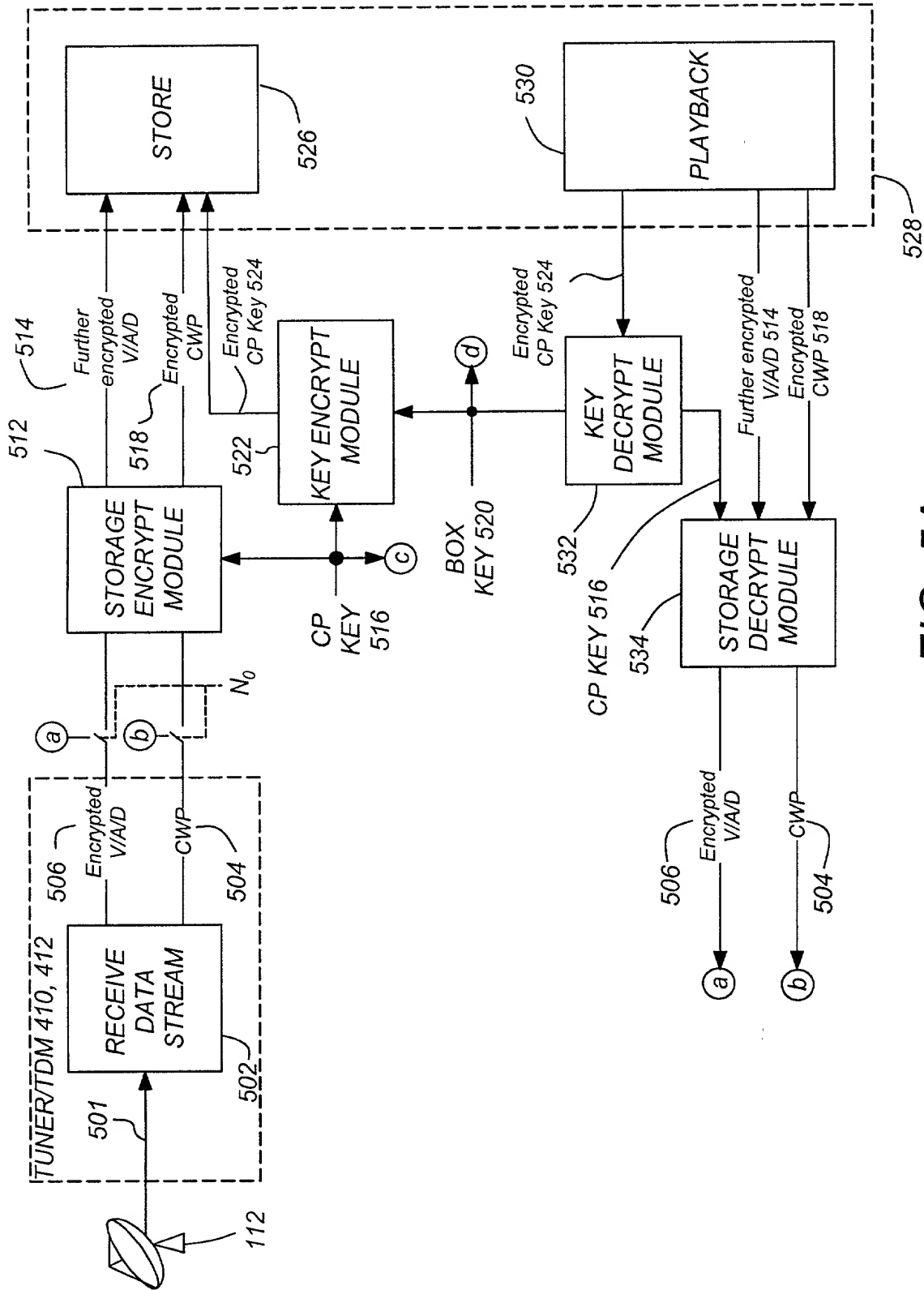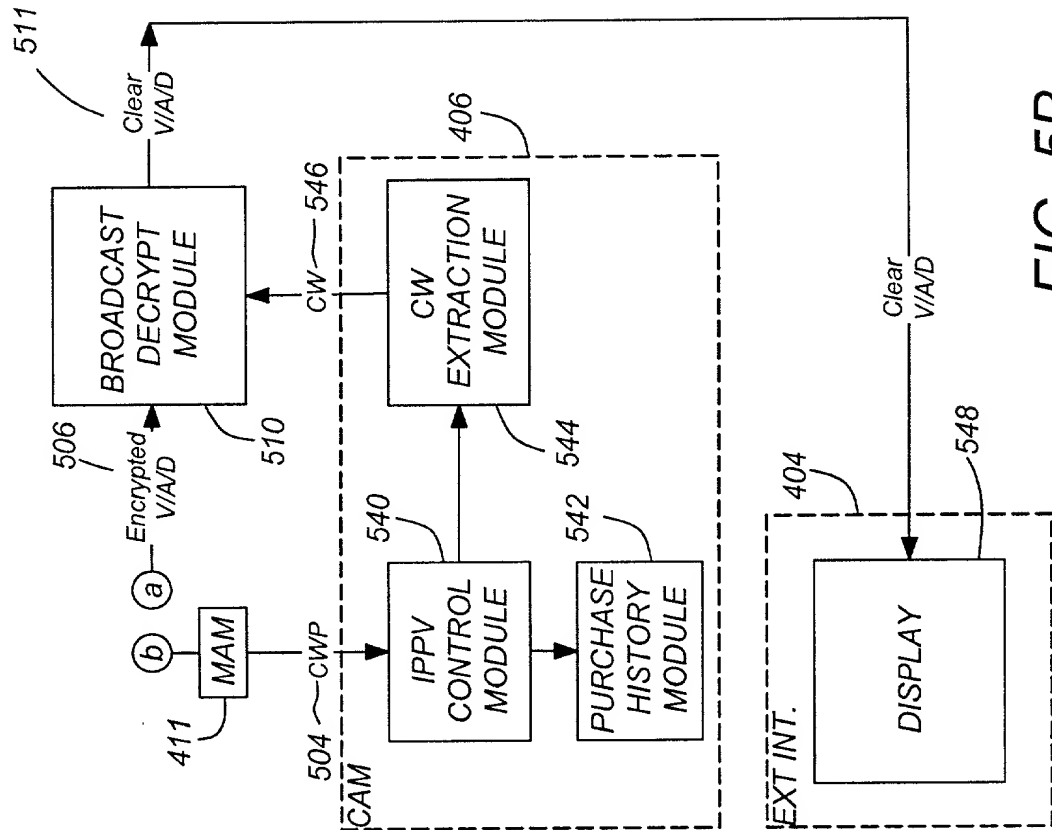
FIG. 5C

United States Patent & Trademark Office
Office of Initial Patent Examination -- Scanning Division

Application deficiencies were found during scanning:

☒ Page(s) _23_ of _the specification_ were not present
for scanning.   (Document title)

☐ Page(s)_____ of _____ were not present
for scanning.   (Document title)

☐ Scanned copy is best available.